**FACEBOOK, INC.**

**Moderator: Tom Reynolds**
**October 12, 2018**
**1:00 p.m. ET**

Operator: Hello and welcome to today's Facebook Press Call. There will be prepared remarks and a Q&A to follow. To ask a question after the prepared remarks conclude, please press "star," "one."

Now, I'd like to turn the call over to Tom Reynolds, who will kick this off.

Tom Reynolds: Thanks, operator, and thanks, everybody, for joining us today.

It's Tom Reynolds from the Facebook Communications team. Joining me here is Guy Rosen, Vice President of Product Management, who oversees safety and security here at Facebook.

Guy's going to give an update on our investigation into the security vulnerability we discovered about two weeks ago, then we'll open it up for questions. And when you ask your question, just a request that you state your name and your publication.

One reminder, this is on the record with no embargo.

With that, let me turn it over to Guy to get us started.

Guy Rosen: Thanks, Tom, and thanks, everyone, for joining us today. Since we announced the security vulnerability two weeks ago, our investigation has focused on understanding as much as we can. We've been looking at how the vulnerability was exploited and what information attackers may have accessed.

Today, we're sharing an update on this investigation. First, I'd like to walk through the timeline and explain how we got here. On September 25 -- that's just over two weeks ago -- we determined that an unusual spike in activity which we had seen earlier and were investigating was actually an attack.

That attack started on September 14th, and it exploited a vulnerability in our code that had existed since July of 2017. That vulnerability was the result of a complex interaction of three bugs in our software. It involved a feature called View As, which people can use to see what their profile looks like to someone else, and with it an attacker could steal what are known as access tokens.

These are like digital keys that keep you logged into Facebook so that you don't need to reenter your password every time you use the app. With these access tokens, an attacker could get into people's accounts.

Within two days of identifying this as an attack, by September 27th, we had closed the vulnerability, we stopped the attack, and we secured people's accounts by resetting the access tokens for people who were potentially exposed.

We also notified the FBI; they've asked us not to share any additional details at this point that could compromise their investigation.

But let's get to what we can share today. We now know that fewer people were impacted by this attack than we originally thought. We found that about 30 million people had their access tokens stolen; that's down from the 50 million we originally feared were affected.

We've also identified how the attack was carried out and what information the attackers were able to access. I'll explain how, and I'll focus on three groups of people. First, the attackers already controlled a set of accounts, so imagine these as seed accounts which were connected to friends on Facebook.

The attackers stole their friends' access tokens, then the access token of the friends of their friends, and so on and so forth. They moved from account to

account using an automated script collecting tokens, repeatedly exploiting the vulnerability using access tokens for about 400,000 people.

In the process, this script automatically loaded those accounts' Facebook profiles, essentially mirroring what these 400,000 people would have seen when looking at their own profiles in a web browser. That would have included things like posts on their Timelines, their list of Friends, Groups they're members of, and the names of some recent Messenger conversations.

Message content was not available to attackers -- with one exception, though. If a person in this group of 400,000 people was a Page admin whose Page had received a message from someone, the content of that message may have been loaded. That's our first group.

They then used the list of friends they collected to eventually steal access tokens for about 30 million people. The second group includes about 15 million people. The attackers accessed two sets of information from them -- their name and contact details. That would have been things like phone numbers or e-mails, depending on what people had on their profiles.

And our third group includes about 14 million people. The attackers were able to access the same information as the second group, plus other details these people had on their profiles. We've posted a full list in our Newsroom and in our Help Center. It included things like gender, relationship status, their birth date, recent searches, and the last 10 places the person had checked into or were tagged in.

We have a tool in our Help Center that people can now use to see whether they were affected, what information may have been accessed. And all of these people across all the groups will get a customized message from us in the coming days. We'll be explaining what information the attackers may have accessed as well as steps they can take to help protect themselves from any suspicious e-mails or text messages or calls that could potentially result from this kind of information being exposed.

And I want to reiterate that people's accounts have already been secured by the action we took two weeks ago to reset the access tokens for people who

were potentially exposed. No one needs to log out again and no one needs to change their passwords.

Our investigation has also shown that the attack did not include Messenger, Messenger Kids, Instagram, WhatsApp, Oculus, Workplace, any third-party apps, payments, Pages, or advertising or developer accounts. And as we said previously, people's credit card information would not have been visible to the attackers, as we do not display full credit card numbers -- not even to the account holder.

We are still looking at other ways the people behind this attack may have used Facebook and we haven't ruled out the possibility of smaller-scale, low-level access attempts during the time the vulnerability was exposed. Our investigation into that continues.

We've been cooperating with the FBI, the US Federal Trade Commission, the Irish Data Protection Commission and other authorities. We will continue to do so as the investigation continues.

People's privacy and security is incredibly important and we are sorry this happened. We know that we will always face threats from those who want to take over accounts or steal information. And that is why we are continuing to invest so heavily in security and focusing on more proactive ways to protect people. We are fully committed to this work and we are going to do all we can to earn people's trust.

Tom Reynolds: Great. Thanks a lot, Guy.

With that, Operator, we can open up to questions. And I would just ask that people state their name and their outlet.

Operator: We will now open the line for questions. Please limit yourself to one question per person. To ask a question press "star" followed by the number "one."

Your first question comes from Donie O'Sullivan of CNN. Your line is open.

Donie O'Sullivan: Hey, folks. Donie O'Sullivan here at CNN.

Can you explain the 400,000 users whose accounts were already accessed, how did they gain access to those accounts and what level of access that they have?

Guy Rosen: Thanks for the question.

The 400,000 accounts were accessed in the same way as the others -- through this vulnerability. The attackers started with a set of accounts they controlled directly and then they moved from them using the vulnerability to their friends and to their friends' friends, and so forth -- each time by stealing the access tokens. The 400,000 accounts are the ones where their script loaded the View As view that actually loads the Facebook profile for that person.

And as part of that, when that webpage loads and renders in their script, it would have included the information that we provided -- things like their posts on their Timeline, list of friends, their Groups they're members of. And as part of that, that information was loaded. We have no reason to believe the attackers were interested in that information; they were running that in order to get the access tokens for those people's friends.

Operator: Your next question comes from Martin Untersinger of Le Monde. Your line is open.

Martin Untersinger: Hi. Thank you for taking my question.

How can you say that the vulnerability is less serious than you thought when you said last time you didn't know if personal data was accessed, and that now you're saying that 29 million plus 400,000 people have had their data accessed?

Guy Rosen: This is a very serious matter and our investigation has been working around the clock to understand how data with accessed and what information was taken, and we're sharing what we have found today.

Operator: Your next question comes from Josh Constine of TechCrunch. Your line is open.

Josh Constine: Is there information about what happened once hackers actually accessed these Profiles, such as if there's any evidence that data was scraped or exported in any way?

Guy Rosen: Hey, Josh.

Once the attackers accessed profiles using these access tokens, the information that they scraped was the information that we shared. For the 400,000 people, certain types of information, for the second group of 15 million people, some basic Profile information, and for the third group of 14 million people, they scraped additional information that is on people's Profiles.

Operator: Your next question comes from Sarah Frier of Bloomberg. Your line is open.

Sarah Frier: Hi. Thank you.

I'm wondering if there's any more clarity on any patterns that you might've seen either in terms of who the attackers were or geographically where they were located and who they were trying to target?

Guy Rosen: We are cooperating with the FBI on this matter; the FBI is actively investigating and have asked us not to discuss who may be behind this attack.

Operator: Your next question comes from Mike Isaac of the New York Times. Your line is open.

Mike Isaac: Thanks. Hey, Guy. This is Mike here from the Times.

I just wanted to ask how you all are able to contact folks who might've actually deleted their accounts before this or folks who had deleted it after, I guess, if you need to like, update them on anything -- if there's a way to contact people that have deleted their accounts?

And I'm just wondering if there's any clarity on the third-party connected apps -- if you all have gotten anywhere on that?

And I apologize if I missed that if you already gave an update.

Guy Rosen: Hey, Mike.

On your first question, first of all, we will be notifying people through Facebook so that they can understand what information was accessed from their account and which group they were part of. We will also work to contact people who may not be on Facebook any longer.

On your second question on third-party apps, we've confirmed that there's no evidence that these attackers accessed third-party apps using Facebook login and actually any developer who uses our official Facebook SDKs as well as any developers who regularly check the validity of the Facebook access tokens that they get were automatically protected two weeks ago when we reset people's access tokens.

Last week, out of an additional abundance of caution, we also built a tool to enable developers to manually identify any users of their apps who may have been exposed, so that they can conduct their own investigations. And if they decide to do so, they can log them out of their services as well.

Operator: Your next question comes from Paresh Dave of Reuters. Your line is open.

Your line is open; you may be on mute.

Your next question comes from Julia Boorstin of CNBC. Your line is open.

Julia Boorstin: Hi.

I'm just wondering if you could tell us if you know anything about what the intention of the hackers was? You mentioned that you can't say what countries they were connected to, but anything about what they were looking to do with this data or how they were looking to exploit it?

And then also if you've seen any other evidence of increased hacker attacks leading up to the midterms or there anything tied to that?

Guy Rosen: As I've said, these are the kind of questions we are working on in this investigation cooperating with the FBI. They're actively investigating this

with us and they've asked us not to discuss who may be behind this attack or what their intentions could be.

On your second question, we are constantly working and have a lot of teams focused on activities ahead of the midterm elections. We have no reason to believe this specific attack was related to the midterms but, unrelated, that is a big focus for all of us here at Facebook from top to bottom. And we have many teams focused on ensuring that we can protect the security of the upcoming elections as well as all other elections around the world.

Operator: Your next question comes from David McCabe of Axios. Your line is open.

David McCabe: Hi, Guy. Thanks so much for holding the call.

I'm wondering, when this was first announced and all you said was these access tokens had been stolen, you were asked -- or Mark was asked -- why should users continue to trust Facebook with their data? And essentially the answer was, we're working really hard to solve this. And I'm wondering if now that users actually know the kind of really personal nature of some this data -- their searches, locations they've been tagged in -- I'm wondering if that answer has changed.

How would you answer that question now that they know the specifics of what was accessed?

Now that they know that info was accessed, why should they continue to trust Facebook with their data?

Guy Rosen: Hey, thanks for the question.

We take these incidents very, very seriously and nothing is more important to us than the security of people's information and that's how we've approached this investigation. That's why we took immediate action to secure people's accounts. That's why we are coming forward consistently to explain what we have learned and as a company, we are investing a lot in safety and security.

This year we are going from 10,000 to 20,000 people, working across all of safety and security. And we know adversaries will always be interested in services like ours. That's why it's very important for us to invest in this and to make sure that we can improve our detection capabilities and we can strengthen our defenses.

Operator: Your next question comes from Danny Fortson of Sunday Times. Your line is open.

Danny Fortson: Hi. Thanks. I just had a couple questions.

Do you have any clarity as to how many U.K. and other European citizens had their data accessed?

And also, what is your interaction with the authorities in the E.U.? Has there been any discussion of potential fines that might arise from this -- from the breach?

Guy Rosen: Hey. Thanks for the question.

We're not sharing any country breakdowns at this time. We are working very closely with regulators and with policymakers around the world to provide them with the information that they need and to respond to their questions.

Operator: Your next question comes from Dan Goodin of Ars Technica. Your line is open.

Dan Goodin: Yes, hi. Thanks.

I just wanted to get clarity on sites that use Facebook for login. Is that part of the third-party apps that you say weren't affected or is that different?

Also, how could attackers access 30 million accounts without triggering some kind of alert from Facebook? Were they using VPNs or botnets or other things to disperse the IPs that were checking these accounts?

Thank you.

Guy Rosen: Thanks for the questions.

On your first question, yes, when I mentioned our findings on third-party apps, that includes websites that use Facebook Login, and our investigation has not found any evidence that the attackers accessed any third-party apps or used Facebook Login.

On your second question, the attack was anomalous and it is what triggered our investigation. And as a result of that investigation into that unusual spike of activity, we looked into that, and when we found just over two weeks ago that this was, in fact, an attack, we moved extremely fast -- within a couple of days -- to fix the vulnerability and to protect the security of people's accounts.

Operator: Your next question comes from Will Oremus of Slate. Your line is open.

Will Oremus: Thanks very much.

All this personal information seems like it could be useful fodder for follow-up hacks of various sorts, spear phishing or identity theft or that sort of thing. Have you seen these signs of that impact happening? And apologies -- I cut out for a bit -- if somebody else asked that already.

Guy Rosen: Hey, Will. Thanks for the question.

We don't have a specific indication of the intention of the attackers. And as we've said, we're cooperating with the FBI in an active investigation. As part of the information that we will be sharing with users over the coming days, we will be including information as to how they can watch out for any suspicious e-mails or text messages or things of that sort.

Operator: Your next question comes from Laura Hautala of CNET. Your line is open.

Laura Hautala: I'm wondering if you can just explain a little bit more about how in the first -- the group of 400,000, I'm just trying to clarify -- those were folks who were associated with the actual accounts that ran the attack? They were there first and second degree friends? Is that correct?

Guy Rosen: Hey, thanks for the question.

The very first seed accounts are likely accounts that are associated with the attackers themselves. And then they went to their friends and their friends of friends, and used the access tokens to essentially login as them and use the vulnerability to get further information. Those initial 400,000 are if you will closer to the original seed accounts -- the small handful of accounts that the attackers started from.

Operator: Your next question is from Tamsin McMahon of The Globe and Mail. Your line is open.

Tamsin McMahon: Hi. Thanks very much for organizing this call. Tamsin McMahon, from The Globe and Mail.

I know you mentioned earlier that you weren't providing a country breakdown at this time. But I wonder if you can kind of give a ballpark of just how broad base -- in terms of geography -- this attack was? Are you talking about dozens of countries? Was it clustered in some handful of countries?

And I was also curious that, I know you've mentioned that these access tokens -- that the attackers were able to steal these access tokens and that these tokens are used for people to have the convenience not to login over and over again on multiple devices. I'm wondering if you considered getting rid of that feature, because it seems that as much as that's an inconvenience it's a relatively small price to pay for people to protect their private information?

Thank you.

Guy Rosen: Hey. Thanks for the question.

On your first point, the attack was fairly broad; I can say that. And as I've said, though, we can't share anymore specific country information at this point.

On your second point, any software that interacts with a service has some form of access tokens that are used once any application is authenticated with a server. We are learning from this incident, we're looking at approaches that

could address this class of problem and ensuring that we can catch them faster and minimize their impact.

Operator: Your next question comes from Octavio Castillo of El Universal. Your line is open.

Octavio Castillo: Hi, guys.

My question was about the country breakdown, but I think it was already answered so I give my turn to the next colleague. Thank you.

Operator: Your next question comes from Soo Youn of ABC News. Your line is open.

(Soo Youn): Hi. Thanks for the call.

I was wondering, you had said earlier that the full credit card information isn't visible even to the user, but would it be the last four digits that would be -- would've been visible?

Guy Rosen: Hey. Thanks for the question. Yes. The user, if they logged in, a user can see their own last four digits. We don't have any evidence that the attackers specifically took any of this information.

Operator: Your next question comes from Ed Ludlow of Bloomberg Television. Your line is open.

Ed Ludlow: Yes. Hi, guys. Thanks for doing the call. Ed Ludlow, from Bloomberg Television.

You said you'd notify users on steps they can take. Have you seen any behavior of how data is being used, or any evidence on the dark web for example that data that was taken during the hack is already being used? Have any users contacted you to say they've been contacted by a suspicious third parties or anything like that?

Thanks.

Guy Rosen: Thank you for the question.

We haven't seen any evidence of this being used yet. We're continuing this investigation and working closely with the FBI to understand and work with their investigation.

Operator: Your next question comes from Dave Ingram of NBC news. Your line is open.

David Ingram: Hey, guys.

If I understood you earlier, Guy, you have a pretty good sense that this attack started with these people's own accounts and people close to them and it grew to the 400,000 from there. Is it fair to say that Facebook now has a pretty good idea of who is behind this attack but cannot at the request of the FBI isn't saying just yet who that is?

Guy Rosen: As I've said, we are working very closely with the FBI; they're actively investigating and they've asked us not to discuss who may be behind this attack.

Tom Reynolds: Operator, we're going to have time for two more questions, please.

Operator: Your next question comes from Paresh Dave of Reuters. Your line is open.

Paresh Dave: Hi there.

Did the attackers have the ability to post as users? And did they post things, and what happened to the other 20 million from the original 5 million estimate?

Guy Rosen: Thanks for the questions.

Based on our investigation, the attackers did not post anything on people's Profiles. The specific kinds of activity and the information that they accessed is the thing that we were sharing today and that we've listed. Our investigation obviously continues.

On your second question -- can you remind me what the second question was? Oh OK, you asked what happened to the other 20 million, sorry. We moved extremely fast two weeks ago to understand all of the users that were exposed to the vulnerability and users that may have been affected by this attack. As a reminder, we reset the access tokens for a total of 90 million users, of which at the time we thought that 50 million were affected by this attack.

Over the course of the investigation in the past two weeks we have confirmed that this attack has affected 30 million people.

Tom Reynolds: Operator, this is going to be our last question.

Operator: Your final question comes from Steven Levy of WIRED. Your line is open.

Steven Levy: Yes. Thanks for doing these calls, guys.

In between September 14th to September 25th when you were doing the investigation, do you think that most of the theft took place during that time? Was there any thought of like turning stuff off or doing anything about that? I mean, are you looking at in the future things to do when you see activity and identifying what the activity is?

Guy Rosen: Hi. Thanks for the question.

The activity took place between, as you said, September 14th until we shut it off. There was a spike in activity. These things do happen. There is always variation in how Facebook is used over the course of any given day. This was unusual and which is what triggered this investigation and prompted us to dig and understand what was going on and eventually uncover that this was, in fact, a security issue. And then we moved extremely fast to be able to fix the vulnerability to secure people's accounts and to share what we had found.

We are continuing to learn and understand what additional tools and what additional measures we take in order to ensure that we can not just address this class of problem -- problems will always happen -- but ensuring that we can move very fast to detect and very fast to address any problems that may occur.

Tom Reynolds: Thanks, Guy.

With that, we're going to conclude. I just want to note that we do have a Newsroom post -- our blog that we posted about 30 minutes ago. We're also going to have the transcript and Q&A posted in the Newsroom as well as soon as possible. And if you have additional follow up questions you can e-mail us at press@fb.com.

Thanks again for your time today.

Operator: This concludes the Facebook Press Call. Thank you for joining. You may now disconnect your line.

END